

Actividad Tipos de Amenazas

Utilizando este documento de presentación, cada mesa deberá resolver y completar en cada hoja , que le corresponde según su número de mesa.



Mesa 3

Nota : <https://www.welivesecurity.com/la-es/2021/04/08/vyveva-nuevo-backdoor-grupo-apt-lazarus/>

¿Qué tipo de amenaza es? Malware, backdoor

¿Cómo comienza y cómo se propaga esta amenaza? El backdoor, principal componente de Vyveva, se conecta a los servidores de C&C y ejecuta los comandos emitidos por los atacantes.

¿Hay más de una amenaza aplicada ? Si. Ejecución, persistencia, evasión de defensa, descubrimiento, colección, comando y control, exfiltración.

¿Qué solución o medida recomendarían ? Descargar un antivirus.